

ABSTRACT

Clocks used by network security devices can be synchronized by a network security system. In one embodiment, the synchronization can include the network security system receiving a first stream of alerts from a first network security device having a first clock, each alert in the first stream representing an event detected by the first network security device and including a time of detection by the first network security device according to the first clock. Similarly, the network security system can receive a second stream of alerts from a second network security device having a second clock, each alert in the second stream representing an event detected by the second network security device and including a time of detection by the second network security device according to the second clock. The system can then identify a common event represented by a first alert in the first stream from the first network security device and by a second alert in the second stream from the second network security device, and then synchronize the first clock and the second clock using the common event.